# Privacy-Aware UAV Flights through Self-Configuring Motion Planning

## Conference or Workshop Item

# Privacy-Aware UAV Flights through Self-Configuring Motion Planning

Yixing Luo[1], Yijun Yu[2], Zhi Jin[1], Yao Li[3], Zuohua Ding[3], Yuan Zhou[4] and Yang Liu[4]

***Abstract*— During flights, an unmanned aerial vehicle (UAV) may not be allowed to move across certain areas due to soft constraints such as privacy restrictions. Current methods on self-adaption focus mostly on motion planning such that the trajectory does not trespass predetermined restricted areas. When the environment is cluttered with uncertain obstacles, however, these motion planning algorithms are not flexible enough to find a trajectory that satisfies additional privacy-preserving requirements within a tight time budget during the flights. In this paper, we propose a privacy risk aware motion planning method through the reconfiguration of privacy-sensitive sensors. It minimises environmental impact by re-configuring the sensor during flight, while still guaranteeing the safety and energy hard constraints such as collision avoidance and timeliness. First, we formulate a model for assessing privacy risks of dynamically detected restricted areas. In case the UAV cannot find a feasible solution to satisfy both hard and soft constraints from the current configuration, our decision making method can then produce an optimal reconfiguration of the privacy-sensitive sensor with a more efficient trajectory. We evaluate the proposal through various simulations with different settings in a virtual environment and also validate the approach through real test flights on DJI Matrice 100 UAV.**

## I. Introduction

Although Unmanned Aerial Vehicles (UAVs) are promising in commercial and public use, there is a growing fear from customers and stakeholders that the usage of UAVs could lead to the leakage of their private information [1]. One general purpose of the application of UAVs is to collect information about the environment with on-board sensors, e.g., camera, by planning the flight paths properly [2]. However, the risk of privacy leakage arises once personal properties are exposed or private lifes are disturbed during the flight of UAVs [3]. According to the EU's General Data Protection Regulations (GDPR) [4], privacy should be protected by controlling the interference with private space and/or the information transmitted.

Hence, the flights of UAVs over private regions shall be prohibited, and certain privacy-sensitive sensors (e.g., camera) shall be controlled. To achieve the above privacy requirements, several methods have been proposed in literature. Most of them focus on the planning of flight paths that can avoid the intervention with known restricted areas or privacy-sensitive regions [5], [6] because the effectiveness of path planning for conflict avoidance with various constraints has been well demonstrated [7], [8]. Additionally, due to the limitations of tasks, motion space, and battery capacity, a UAV cannot always find a path satisfying all the privacy requirements using existing motion planning methods [5].

To address the aforementioned problems, we propose an adaptive planning method for motion safety and a self-reconfigurable sensor to guarantee privacy-preservation. It consists of three parts:

1) **Online privacy risk detection and modelling** to handle previously unknown private regions and dynamic privacy demands of citizens;
2) **Real-time motion planning** when the reference flight paths interfere with newly detected private regions; and
3) **Sensor reconfiguration** offers the best possible privacy preservation when there is no feasible flight path to meet the strict privacy requirements for motion safety and task completion.

We also test the effectiveness and performance of the approach through simulations and experiments on a real-life outdoor scenario using a DJI Matrice 100 UAV.

The contributions of this work are summarised as follows:

- We propose a model for the risk assessment of privacy intrusion, which makes UAVs aware of the uncertain and dynamic environment;
- We propose a self-adaptive motion planner for online path generation and sensor reconfiguration so as to always satisfy motion safety, task completion, and privacy requirements.

The rest of paper is organised as follows. Sect. II gives a brief literature review. The problem statement is given in Sect. III. The detailed design of our method is given in Sect. IV. Sect. V describes our simulation results and experiments on real UAV flights. The paper is concluded in Sect. VI.

## II. Related Work

Most existing research focused on motion planning of autonomous systems sharing the environment with the guarantees of *safety* (i.e., the collision shall never happen) and *liveness* (i.e., travel to the destination eventually) [9]–[13]. For example, distributed approaches are proposed in [9], [10] to avoid collisions and deadlocks in multi-robot systems. In more complex scenarios, time, energy, and visibility constraints are taken into consideration [2], [14]. For example, a

*The work is supported in part by the National Natural Science Foundation of China under Grant Nos. 61620106007 and 61751210, the EPSRC platform grant in the UK (SAUSE), ERC Advanced Grant on Adaptive Security and Privacy, and EU H2020 EngageKTN grant on Drone Identity. Zhi Jin is corresponding author.

[1]Yixing Luo and Zhi Jin are with Key Lab. of High Confidence of Software Technologies(MoE), Department of Computer Science and Technology, School of EECS, Peking University, Beijing, China {yixingluo, zhijin}@pku.edu.cn

[2]Yijun Yu is with School of Computing and Communications, The Open University, Milton Keynes, UK {yijun.yu}@open.ac.uk

[3]Yao Li and Zuohua Ding are with School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou, Zhejiang, China {zouhuading}@hotmail.com

[4]Yuan Zhou and Yang Liu are with School of Computer Science and Engineering, Nanyang Technological University, Singapore {y.zhou, yangliu}@ntu.edu.sg

search-based path planning algorithm for safe navigation under visibility constraints has been proposed in [14]. However, privacy preservation for restricted areas is rarely considered in these traditional motion planning methods.

Several methods for privacy protection during flights of UAVs have been proposed in literature. For example, image denaturing techniques [15] are put forward for sensitive data protection. However, they are unrealistic for private users or commercial entities due to the high cost and time consumption [16]. Regulating UAV altitudes and onboard camera capability to reduce video quality is another method [17]; however, it only mitigates privacy threats from the perspective of handling adversarial computer vision attacks while not addressing physical intrusions. Determining the border of a property according to its owner, "privacy by design" principles can be applied to prevent a violation in advance [6], while checking entities are required to gather the information about declarer's identity and to verify the crossing of property borders [3]. With differential permission of UAV given by citizens, a framework for UAV movement under privacy constraints is introduced in [5]. However, direct mapping of geospatial projection and land register information is not generally available where UAVs need to detect private regions online, to adapt the system behaviours and adjust the sensor parameters for privacy preservation.

Autonomous unmanned systems like UAVs are controlled by software with self-adaptive planning methods [18], which decides the planning and subsequent actions in response to uncertainty in the dynamic environment. Although models of software and environment have been leveraged for automated adaptation in robotics software [19]–[21], little has been done to guarantee privacy preservation during UAVs' flights. In this work, we proposed a real-time self-adaptive planner which is responsible for task adaptation (e.g., taking an alternate path) and architectural adaptation (e.g., sensor reconfiguration). Based on an updated risk model, the planner optimises the performance in terms of safety and task completion time, while controlling the privacy violation risks.

## III. Motion Modelling and Problem Statement

### A. Motion Modelling

*1) Environment Discretization:* Suppose that in the operating environment of a UAV, there are obstacles and private regions (e.g., properties of people like residential areas) which can be detected by the UAV's onboard sensors, such as camera, Lidar, etc. The UAV should avoid hitting all obstacles compulsorily, while intruding private regions and exposing private information as much as possible. In this work, we discretise the environment into a set of equally-sized grids. Each grid is distinguished by its centre $(x,y,z)$, so the environment can be described as $M = \{p = (x,y,z) | x = \{0,\ldots,X\}, y = \{0,\ldots,Y\}, z = \{0,\ldots,Z\}\}$. Let $O \subseteq M$ and $C \subseteq M$ be the set of grids containing obstacles and private regions respectively. Due to the uncertainty of private areas and the dynamics of privacy requirements, $C$ will be updated online when a new private region $c_m$ is detected by the UAV. The two grids containing the initial and the target locations are denoted as $p_s$ and $p_e$, respectively.

*2) UAV Model:* In this work, a UAV avoids unwanted disclosure of private regions during its motion by adjusting its trajectory and reconfiguration of the onboard camera. Hence, at each time step $t$, the state of a UAV is described as $s_t = [p_t,\ \boldsymbol{ws}]^\top$, where $p_t = (x,y,z) \in M$ is the grid occupied by the UAV at $t$; $\|\boldsymbol{ws}\| \in (0,1]$ is a normalised configuration parameter of the camera's properties, such as orientation angle, resolution, etc. The mission of the UAV is to travel from $p_s$ to $p_e$ within a given time budget. At any time step, the UAV is assumed to move to an adjacent grid in one of the six directions: up, down, right, left, forward, and backward. Hence, the distance of movement from the time step $i$ to $j$ can be computed by the 1-norm distance, i.e., $l_{i,j} = \|p_i - p_j\|_1$. Assuming that the UAV moves at a constant velocity $v$, the travel time needed from $i$ to $j$ is computed as $\tau_{i,j} = l_{i,j}/v$.

### B. Privacy Violation Risk Modelling

Based on the risk assessment methodology adopted by the National Institute of Standards and Technology (NIST) [22], the risk of privacy violations of a given private region $c_m$ can be defined as the product of impact and likelihood. For three intensity levels of residential areas (i.e., sparse, medium, dense), we quantify the harmful impact $h_m$ for privacy violation risk as *high* (semi-quantified as 8 [22]), *moderate* (5), and *low* (2) correspondingly.

Following the safety index map modelling introduced in [23], the possibility of privacy violation risk can be estimated that, the greater the distance between the UAV and the centre of a private region $c_m$, the less possible sensitive information being taken. The affected area of a private region is modelled as concentric spheres with radius $r_{low}$ and $r_{high}$. Hence, the set of all areas affected by private regions can be described defined as risk regions $M_{risk} = \{M_m = (c_m, r_{low}, r_{high}) | c_m \in C\}$. If the distance of the UAV and $c_m$ is larger than $r_{high}$, the privacy risk is ignored; while the distance less than $r_{low}$ is denied due to safety violation. Note that although the camera's parameters can be tuned, for the UAV within $r_{high}$, its noise and visibility may still be viewed as kinds of privacy violation.

Hence, the privacy violation risk for $M_m$ at $s_t$, denoted as $pr((p_t, \boldsymbol{ws}_t), M_m)$, can be computed by the following exponential function:

$$pr((p_t,\boldsymbol{ws}_t),M_m) = \begin{cases} \infty, & d \le r_{low} \\ h_m \exp(-\frac{\|\boldsymbol{ws}\|_t}{2} \cdot d^2), & r_{low} < d \le r_{high} \\ 0, & d > r_{high} \end{cases} \quad (1)$$

where $d = ||p_t - c_m||_2$ is the distance between the center of privacy region $c_m$ and the UAV.

**Problem Statement:** *Given the initial position $p_s$, and the target position $p_e$, an initial camera configuration $\|\boldsymbol{ws}\|_0$, and the time budget $T_b$ of the flight, find an optimal trajectory and camera configuration in real-time so to minimise the privacy violation risk during its motion in an environment containing obstacles and uncertain private regions.*

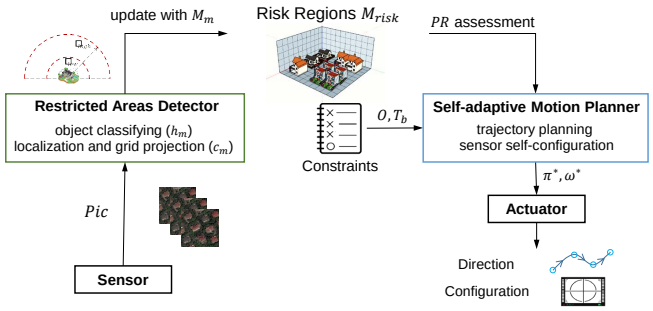



Fig. 1: Architecture of the proposed method.

## IV. Self-Adaptive Motion Planning

This section presents the self-adaptive motion planning framework which generates an optimal trajectory and camera configuration so as to minimise the privacy violation risk under safety and time constraints. An overview of our approach is given before describing the details of each step.

### A. Approach Overview

The architecture for privacy-aware UAV is shown in Fig. 1. During the flight, recordings of the environment *Pic* are captured and saved within the sensing radius $R$ of the onboard camera. Candidates of private regions are identified and projected into the grids of the working space. So the UAV can update risk region $M_m$ new found. With the updated risk regions $M_{risk}$, safety and time constraints, an optimal trajectory $\pi^*$ and camera configuration plan $\omega^*$ are generated locally for the UAV. Furthermore, planning results received by the actuator are converted into mechanical motions.

For real-time private region detection, a UAV first leverages the object detection algorithm YOLOv3 [24] to identify potential private regions based on the captured pictures. The objection detection model is trained with two remote sensing data sets NWPU-RESISC45 [25] and AID [26] for aerial scene understanding. Then a monocular-vision-based method [27] is used to locate their position in the working space $M$. Next, we present the detailed design of the self-adaptive motion planner.

### B. Privacy Aware Motion Planning

At any time step $t$, assuming that the set of risk regions is $M_{risk}$, for a given trajectory $\pi_t = p_{t+1}, \ldots, p_n$, and a camera configuration $\omega_t = \boldsymbol{ws}_{t+1}, \ldots, \boldsymbol{ws}_n$, the accumulated privacy violation risk of $\pi_t$ under $\omega_t$ can be formulated as:

$$PR(\pi_t, \omega_t, M_{risk}) = \sum_{i=t+1}^{n} \sum_{M_m \in M_{risk}} pr((p_i, \boldsymbol{ws}_i), M_m) \tag{2}$$

In time-sensitive scenarios, time to completion is also expected to be minimised. As the UAV is flying at a constant velocity, given the trajectory $\pi_t$, the travel time along $\pi_t$ is $\tau(\pi_t) = \sum_{i=t+1}^{n} \tau_{i,i-1} = \sum_{i=t+1}^{n} \|p_i - p_{i-1}\|_1 / v$. Since in our work, the privacy violation risk is the primary objective during motion planning, we give a constant slack factor $\delta$ to the time budget $T_b$ and a penalty function $\phi(\pi_t)$ to the privacy violation risk, by defining a mixed objective function $\phi(\pi_t) PR(\pi_t, \omega_t^0, M_{risk})$ where $\omega_t^0 = (\|\boldsymbol{ws}\|_0)_{t+1}^n$. In this way, we set $\phi(\pi_t)$ as a piece-wise function for the punishment of overtime:

$$\phi(\pi_t) = \begin{cases} 1, & \tau(\pi_t) \le T_{opt} \\ \eta \exp(\frac{\tau(\pi_t) - T_{opt}}{T_{plan} - T_{opt}}), & T_{opt} < \tau(\pi_t) \le T_{plan} \end{cases} \tag{3}$$

where $\tau_{s,t} = \|p_1 - p_s\|_1 + \sum_{i=1}^{t-1} \|p_{i+1} - p_i\|_1$, $T_{opt} = T_b - \tau_{s,t}$, and $T_{plan} = (1+\delta)T_b - \tau_{s,t}$, $\eta \ge 1$ is a constant. The slack factor and penalty factor encourage the UAV to move to its target within the time limit, but they also allow some delay to guarantee privacy preservation.

Hence, the optimisation problem at time step $t$ to generate the future optimal trajectory under the initial camera configuration $\boldsymbol{ws}_0$ can be described as follows.

$$\begin{aligned} \min_{\pi_t = p_{t+1}, \ldots, p_n} \quad & \phi(\pi_t) PR(\pi_t, \omega_t^0, M_{risk}) \\ \text{subject to} \quad & p_n = p_e; \\ & \tau(\pi_t) \le (1+\delta)T_b - \tau_{s,t}; \\ & p_i \notin O, \ i = t+1, \ldots, n. \end{aligned} \tag{4}$$

This problem can be solved by the $A^*$ algorithm. However, when the motion space is large, the computation time is long, which would not be available for real-time planning. Hence, in this paper, we propose an approximate solution. Although the environment is partially known initially, the UAV could plan a reference trajectory from the initial position to the target position in advance. In this way, at any time step, the trajectory generated at the previous time step is determined. The main idea of our approximate solution is that at the time step $t$, we only replan the trajectory segments in $\pi_{t-1}$ (except current position) that violate the privacy requirements with the new detected private regions. Let $U$ be the set of grids in $\pi_{t-1} = p_t, p_{t+1}, \ldots, p_n$ whose privacy risk is not zero, and $M_{risk}$ be the updated private regions at $t$, then

$$U = \bigcup_{k=t+1}^{n} p_k : \exists M_m \in M_{risk}, pr((p_k, \boldsymbol{ws}_0), M_m) > 0 \tag{5}$$

For the first maximally continuous segment $U_1 = \{p_{i+1}, \ldots p_{j-1}\} \subseteq U$, we replan a new trajectory from $p_i$ to $p_j$ that minimise the privacy violation risk. Let $\tau_{s,i}$ and $\tau_{j,e}$ be the time from $p_s$ to $p_i$ and from $p_j$ to $p_e$, respectively. The time budget for the motion from $p_i$ to $p_j$ is $T'_{opt} = T_b - \tau_{s,i} - \tau_{j,e}$, and $T'_{plan} = (1+\delta)T_b - \tau_{s,i} - \tau_{j,e}$. As $\tau_{i,j}$ is the motion time from $i$ to $j$, penalty function (3) can rewritten as:

$$\phi' = \begin{cases} 1, & \tau_{i,j} \le T'_{opt} \\ \eta e^{\frac{\tau_{i,j} - T'_{opt}}{T'_{plan} - T'_{opt}}}, & T'_{opt} < \tau_{i,j} \le T'_{plan}. \end{cases} \tag{6}$$

And the optimisation problem (4) can be rewritten as:

$$\begin{aligned} \min_{p_{i+1}, \ldots, p_{j-1}} \quad & \phi' \sum_{k=i+1}^{j-1} \sum_{M_m \in M_{risk}} pr((p_k, \boldsymbol{ws}_0), M_m) \\ \text{subject to} \quad & \tau_{i,j} \le T'_{plan}; \\ & p_k \notin O, \ k = i+1, \ldots, j-1. \end{aligned} \tag{7}$$

**Algorithm 1:** Sensor configuration based motion planning for a UAV at time step $t$.

**Input:** $\pi_{t-1}, \omega_0, p_t, p_e, T_{budget}$.

1 Initialisation: $\pi_t = \pi_{t-1} - \{p_t\}$ and $\omega_t = \omega_t^0$;
2 Take *Pic* for private regions detection;
3 Update $O$ and $M_{risk}$;
4 Generate $U$ based on (5);
5 **while** $U \neq \emptyset$ **do**
6  Select the first maximal continuous trajectory segment in $U$: $U_1$;
7  Find an optimal solution $\pi^*_{t,1}$ and the optimal value $V^*$ by solving (7);
8  **if** $\pi^*_{t,1} = None$ or $V^* > 0$ **then**
9  Find an optimal solution $\pi^*_{t,2}$ and $\omega^*_t$ by solving (8);
10  Update $\pi_t$ with $\pi^*_{t,2}$ and $\omega_t$ with $\omega^*_t$;
11  **else**
12  Update $\pi_t$ with $\pi^*_{t,1}$;
13  $U = U - U_1$;
14 **return** $\pi_t$ and $\omega_t$;

If (7) generates an optimal solution $\pi^*_{t,1}(p_i \to p_j)$ with the optimal value of zero, then replace the original segment with the optimal one, and compute the next maximally continuous segment in $U$. However, if (7) cannot generate a solution or the optimal value is not zero, then we will adapt to search for an optimal solution with camera reconfiguration.

### C. Sensor Self-configuration

In case the solution of (7) does not guarantee privacy preservation, i.e., the optimal value of (7) is larger than 0, meaning that there is not an ideal path without privacy violation risk, a suboptimal option can be to regulate the onboard camera configuration so as to reduce the potential privacy risk. Hence, we have the following self-configuring motion planning problem:

$$\begin{aligned} \min_{\substack{p_{i+1},\ldots,p_{j-1},\\ \boldsymbol{ws}_{i+1},\ldots,\boldsymbol{ws}_{j-1}}} \quad & \phi' \sum_{k=i+1}^{j-1} \sum_{M_m \in M_{risk}} pr((p_k, \boldsymbol{ws}_k), M_m) \\ \text{subject to} \quad & \tau_{i,j} \leq T'_{plan}; \\ & p_k \notin O, \boldsymbol{ws}_k \succeq \boldsymbol{ws}_0,\ k = i+1, \ldots, j-1. \end{aligned} \tag{8}$$

The solution of (8) is recorded as $\pi^*_{t,2}(p_i \to p_j)$ and $\omega^*_t$.

Compared with (7) and (8), optimizing in a larger search-space, (8) is bound to give a solution that is better than a smaller search-space solution of (7).

Our self-adaptive motion planner is summarised in Algorithm 1. Lines 5−7 perform the first phase, i.e., privacy-preserving motion planning, and Lines 8−10 perform the second phase, i.e., sensor self-configuring motion planning.

## V. Experiments

### A. Simulations

We first validate our approach using simulations under three scales of working spaces, i.e., $10\times10\times10$, $50\times50\times10$ and $100\times100\times10$ grids, cluttered with various density of obstacles $\lambda_o$ and private regions $\lambda_p$. The simulation environment is implemented with Python. Buildings for commercial or industrial use are obstacles and marked in blue, while residential buildings are private regions and marked in red[1]. The depth of colors reflects the height of the building. The starting point is set at the lower-left corner and the target point is set at the upper-right corner marked in yellow. For the $10\times10\times10$ working space, we generate the buildings randomly. The latter two working spaces are abstracted from the open building dataset of Portland in the USA [28]. The final representation is based on a 3D grid so that the map is partitioned into grids, each of which represents a region of $10m\times10m\times10m$ in practice according to the method introduced in [29]. The longitude and latitude of the center of each building, and its average height and building types (apartment, duplex, houses) are also extracted from this dataset. In each working space, the sensibility of UAV is simulated by its view radius $R = \alpha \max_{c\in C} r_{high}(c)$, where $\alpha > 1$ indicates that the UAV can detect private regions proactively. For dense, medium, and sparse residential areas, $r_{high}$ is set to 1, 1.5, and 2 grids respectively, whilst $r_{low}$ is set to 0.5 grid.

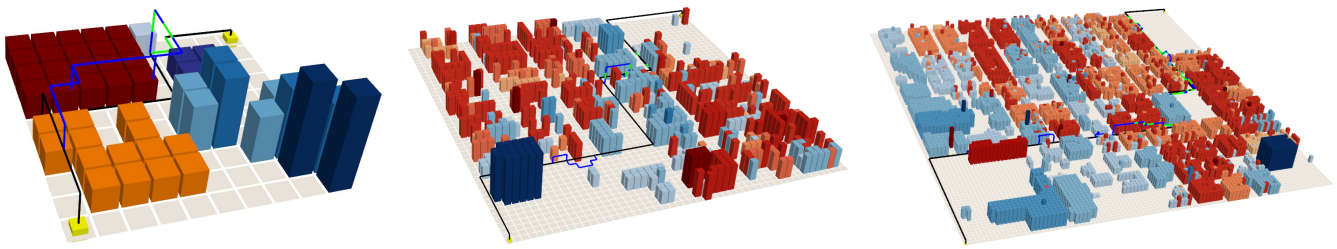
Fig. 2 shows the trajectories generated by our method. In the figure, the black line is the reference path generated off-line; the blue one is generated at the first phase in Alg. 1, while some parts violate privacy requirement, so the second phase tweaks these parts by adjusting both trajectory and camera configuration, i.e., the green parts.

### B. Performance Analysis

To further analyse the efficiency of our Sensor Self-Configuring based Motion Planning (SC-MP) method, we focus on the $10\times10\times10$ working space by setting different obstacle density $\lambda_o$, private region density $\lambda_p$, camera view radius $R$, exploration rate $ER$ (the prior information of the private regions), and time budget $T_b$. We compare our method with the pure Path Planning method (PP) mentioned in [3], which is realised as a variant of the $A^*$ algorithm to avoid private regions at the least privacy risk, and the Sensor Configuration method (SC), which is validated in [17] for privacy protection.

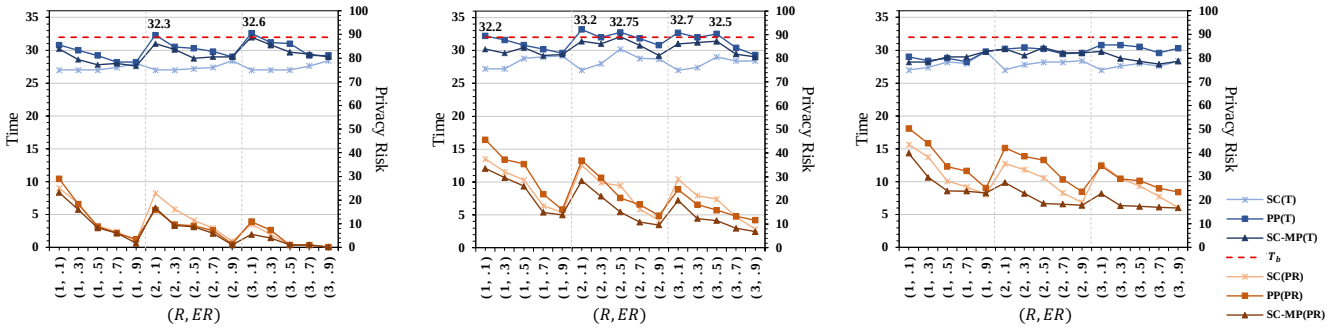
*1) Effect of tuning $\lambda_o$ and $\lambda_p$:* Given the time budget $T_b = 32$ time steps and the slack factor $\delta = 0.125$, we vary the densities of obstacles and private regions, i.e, $\lambda_o$ and $\lambda_p$, in the working space. For each combination, we record the generated trajectories and time to completion with different view radius and exploration rate. As illustrated in Fig. 3, our method SC-MP generates trajectories with the lowest accumulated privacy violation risk $PR$ and middle task completion time $\tau_{s,e}$ in different settings. Comparing with the privacy violation risk shown in Figs. 3(a) and 3(b), it can be found that with an increase of $\lambda_p$, SC-MP registers lower average mission completion time than PP and outperforms the other two methods in privacy preservation. This implies

[1]In black/white prints, red shapes are darker than blue one, green line segments are lighter than the black ones.



(a) $10 \times 10 \times 10$ grid map ($R = 2$) (b) $50 \times 50 \times 10$ grid map ($R = 4$) (c) $100 \times 100 \times 10$ grid map ($R = 4$)

Fig. 2: Planning results for self-adaptive motion planning at different scales of grids.




(a) $\lambda_o = 0.2$, $\lambda_p = 0.05$ (b) $\lambda_o = 0.2$, $\lambda_p = 0.1$ (c) $\lambda_o = 0.3$, $\lambda_p = 0.1$

Fig. 3: Mission completion time and privacy violation risk with various sensibility and scenario settings.

TABLE I: Probability of Privacy Intrusion with $\lambda_o = 0.3$, $\lambda_p = 0.1$, $T_b = 32$, $\delta = 0.125$

| ***Strategies*** | $R = 1$ | | $R = 2$ | | $R = 3$ | |
|---|---|---|---|---|---|---|
| | $ER$=0.3 | $ER$=0.7 | $ER$=0.3 | $ER$=0.7 | $ER$=0.3 | $ER$=0.7 |
| SC | 63.12% | 45.54% | 53.17% | 42.66% | 49.49% | 39.73% |
| PP | 56.00% | 39.07% | 45.51% | 34.52% | 37.58% | 31.48% |
| ***SC-MP*** | ***47.00%*** | ***35.02%*** | ***39.66%*** | ***32.90%*** | ***33.80%*** | ***28.95%*** |

TABLE II: Probability of Camera Configuration and Trajectory Replanning with $\lambda_o = 0.2$, $\lambda_p = 0.1$, $R = 3$, $ER = 0.5$

| ***Strategies*** | ***Camera Configuration*** | | ***Trajectory Replanning*** | |
|---|---|---|---|---|
| | $T_b = 30$ | $T_b$=36 | $T_b$=30 | $T_b$=36 |
| SC | 48.03% | 46.75% | / | / |
| PP | / | / | 28.03% | 33.97% |
| ***SC-MP*** | ***44.10%*** | ***40.98%*** | ***23.25%*** | ***30.58%*** |

that our method is suitable for the environment clustered with private regions. From Figs. 3(b) and 3(c), we can find that as the density of obstacles increases, the mission completion time does not vary greatly, and the PP method is more likely to finish its mission on time. This is because the UAV cannot change its trajectories greatly to guarantee safety in an environment cluttered with obstacles. In such environments, performance for privacy-preservation is also sacrificed for the safety reason, whereas the benefits of more prior knowledge ($ER \geq 0.5$) is not obvious.

*2) Effect of tuning R and ER:* The ability to be aware of the environment is affected by the capability of the camera or other sensors the UAV equipped with (e.g., Lidar). From each sub-figure in Fig. 3, we found that under our method, the increasing of $R$ contributes to lower privacy violation risk but a longer path. This is because, with more private regions detected proactively at each time step, SC-MP prefer to make an adaptive plan to avoid private regions intrusion. Table I also shows the probabilities of trespassing into a private region with different view radius under different methods. We found that our method has the lowest probabilities of intrusion since our method avoids private regions by changing both trajectories and camera configuration. Sensor parameters can be tuned for a compromise under the time constraint in SC-MP, while SC suffers from the highest probabilities of private region intrusion since it does not change the waypoints listed in the reference trajectory. As shown in Fig. 3, the privacy violation risk decreases when more prior knowledge of private regions is acquired before the flight. This is because we can plan a more privacy-aware reference trajectory off-line with such information. However, at a higher view radius ($R = 3$), the benefit of having more prior knowledge is not significant for privacy preservation. The reason is that with a higher view radius, the UAV can detect more private regions online, which has similar effect of more prior knowledge.

*3) Effect of tuning $T_b$:* Time sensitiveness of UAV flight missions varies to applications, e.g., public safety, commercial use like goods delivery, and personal use for entertainment. Table II shows the probability of sensor reconfiguration and trajectory replanning under different values of $T_b$. When $T_b$ increases, the probability of sensor reconfigured decreases for both SC-MP and SC, while the possibility of trajectory replanning increases for SC-MP and PP. Indeed, with the increase of time budget, the UAV has more time redundancy, so it can change the trajectory to be away from private regions. This can eliminate privacy violation risk by avoiding

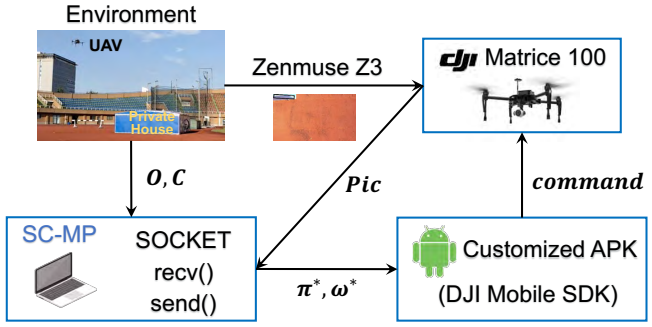



Fig. 4: Architecture of the experiment setup.

the physical intrusion into those regions.

From the analysis above, it can be concluded that our proactive and online method (SC-MP) is suitable for different environments and outperforms methods of pure path planning and sensor configuration in privacy preservation.

### C. Experiments On A Real UAV

We implement the algorithm on a Lenovo laptop to control a DJI Matrice 100 UAV equipped with camera Zenmuse Z3, whose resolution ranges from $4096 \times 2160$ to $1920 \times 1080$, and the orientation angle $\theta$ ranges from $-90^\circ$ to $30^\circ$. The laptop is equipped with Intel(R) Core(TM) i7-7500U CPU@2.70GHz and NVIDIA GeForce 940MX. The architecture of the experiment setup is depicted in Fig. 4. First, the onboard camera of UAV checks the current environment and sends the captured pictures to the laptop for private region identification and localisation. Then the algorithm computes a new trajectory and camera configuration based on the current environmental conditions and sends to the UAV for execution via a customised Android application deployed on a remote controller.

The experiments are conducted in a $10m \times 10m$ outdoor environment with a maximum height of 5m. The private region is marked as a blue box on the playground, while its location is estimated based on the pictures taken by the UAV. During its flight, the UAV replans a trajectory and adapts its camera's orientation for privacy preservation. Under the proposed approach, privacy risk was reduced by 85.32% against the reference path with $T_b = 24$ time steps and $\delta = 0.083$. Figs. 5 and 6 show some snapshots during the motion of the UAV with the reference path and with self-adaptation, respectively. Without the proposed algorithm, the UAV can always "see" the private region while crossing it. To prevent taking pictures of the blue box, the UAV changes its trajectory and alters its camera's orientation from $-90^\circ$ to $30^\circ$, while considering the tight time budget based on our method. The videos of our simulations and outdoor experiments are given at `https://yixingluo.github.io/SCMP.github.io/`.

## VI. CONCLUSIONS AND FUTURE WORK

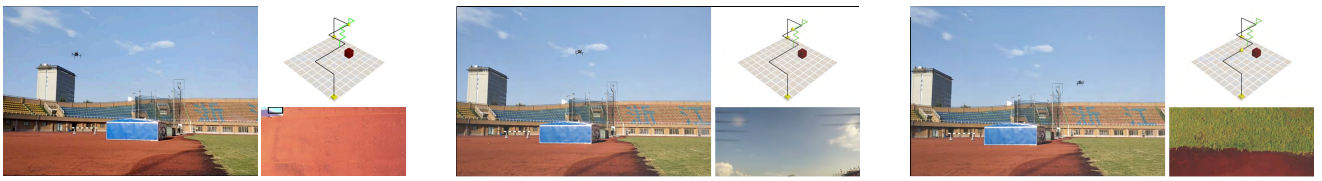
Aiming at privacy-aware motions of UAVs with uncertain private regions or dynamic privacy requirements, this work presents a motion planning algorithm with self-reconfiguration of privacy-sensitive sensors. Within a space modelled with 3D grids, the algorithm generates the optimal UAV motion plan for a privacy-preserving trajectory and sensor configuration with the least privacy risk. The proposed approach has been validated experimentally through both simulations and test flights of a physical UAV. The results demonstrated the effectiveness and efficiency of the method. Future work will take into considerations multiple aspects, including the kinematics of the UAV, more parameters of on-board sensors for self-configuration, and various kinds of environment disturbances.

## REFERENCES

[1] R. D'Andrea, "Guest editorial can drones deliver?" *IEEE Transactions on Automation Science and Engineering*, vol. 11, no. 3, pp. 647–648, 2014.

(a) The first time the private region is detected. (b) The private region is always in sight. (c) The UAV passes through the private region.

Fig. 5: Snapshots of the UAV moving along the reference trajectory without our method.



(a) The UAV detects the private region and replans its trajectory and camera orientation. (b) The private region is avoided by changing trajectory and camera orientation is tuned to 30°. (c) The UAV passes through the private region, and camera orientation is tuned back to $-90^\circ$.

Fig. 6: Snapshots of the UAV moving with our sensor configuration based motion planning method.

[2] M. Popović, G. Hitz, J. Nieto, I. Sa, R. Siegwart, and E. Galceran, "Online informative path planning for active classification using UAVs," in *Proceedings of 2017 IEEE international conference on robotics and automation (ICRA)*, 2017, pp. 5753–5758.

[3] P. Blank, S. Kirrane, and S. Spiekermann, "Privacy-aware restricted areas for unmanned aerial systems," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 70–79, 2018.

[4] P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, 1st ed. Cham, Switzerland: Springer, 2017.

[5] H. Kim, J. Ben-Othman, and L. Mokdad, "UDiPP: A framework for differential privacy preserving movements of unmanned aerial vehicles in smart cities," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3933–3943, 2019.

[6] Y. Pan, S. Li, J. L. Chang, Y. Yan, S. Xu, Y. An, and T. Zhu, "An unmanned aerial vehicle navigation mechanism with preserving privacy," in *Proceedings of 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[7] L. Babel, "Coordinated target assignment and UAV path planning with timing constraints," *Journal of Intelligent & Robotic Systems*, vol. 94, no. 3-4, pp. 857–869, 2019.

[8] Y. Zhou, H. Hu, Y. Liu, S.-W. Lin, and Z. Ding, "A real-time and fully distributed approach to motion planning for multirobot systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2017.

[9] Y. Zhou, H. Hu, Y. Liu, and Z. Ding, "Collision and deadlock avoidance in multirobot systems: A distributed approach," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 7, pp. 1712–1726, 2017.

[10] Y. Zhou, H. Hu, Y. Liu, S.-W. Lin, and Z. Ding, "A distributed method to avoid higher-order deadlocks in multi-robot systems," *Automatica*, vol. 112, p. 108706, 2020.

[11] ——, "A distributed approach to robust control of multi-robot systems," *Automatica*, vol. 98, pp. 1–13, 2018.

[12] S. Liu, M. Watterson, K. Mohta, K. Sun, S. Bhattacharya, C. J. Taylor, and V. Kumar, "Planning dynamically feasible trajectories for quadrotors using safe flight corridors in 3-d complex environments," *IEEE Robotics and Automation Letters*, vol. 2, no. 3, pp. 1688–1695, 2017.

[13] E. Yel, T. X. Lin, and N. Bezzo, "Self-triggered adaptive planning and scheduling of UAV operations," in *Proceedings of 2018 IEEE International Conference on Robotics and Automation (ICRA)*, 2018, pp. 7518–7524.

[14] M. Nieuwenhuisen and S. Behnke, "Search-based 3d planning and trajectory optimization for safe micro aerial vehicle flight under sensor visibility constraints," in *Proceedings of 2019 International Conference on Robotics and Automation (ICRA)*. IEEE, 2019, pp. 9123–9129.

[15] J. Wang, B. Amos, A. Das, P. Pillai, N. Sadeh, and M. Satyanarayanan, "A scalable and privacy-aware IoT service for live video analytics," in *Proceedings of the 8th ACM on Multimedia Systems Conference*. ACM, 2017, pp. 38–49.

[16] A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satyanarayanan, "Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications," in *Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1387–1396.

[17] Z. Li, C. Gao, Q. Yue, and X. Fu, "Toward drone privacy via regulating altitude and payload," in *Proceedings of 2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 562–566.

[18] Y. Luo, Y. Yu, Z. Jin, and H. Zhao, "Environment-centric safety requirements for autonomous unmanned systems," in *Proceedings of 2019 IEEE 27th International Requirements Engineering Conference (RE)*, 2019, pp. 410–415.

[19] J. Aldrich, D. Garlan, C. Kästner, C. Le Goues, A. Mohseni-Kabir, I. Ruchkin, S. Samuel, B. Schmerl, C. S. Timperley, M. Veloso *et al.*, "Model-based adaptation for robotics software," *IEEE Software*, vol. 36, no. 2, pp. 83–90, 2019.

[20] P. Jamshidi, M. Velez, C. Kästner, N. Siegmund, and P. Kawthekar, "Transfer learning for improving model predictions in highly configurable software," in *Proceedings of the 12th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, 2017, pp. 31–41.

[21] P. Jamshidi, J. Cámara, B. Schmerl, C. Kästner, and D. Garlan, "Machine learning meets quantitative planning: Enabling self-adaptation in autonomous robots," *arXiv preprint arXiv:1903.03920*, 2019.

[22] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Tech. Rep., 2012.

[23] Q. Ren, Y. Yao, G. Yang, and X. Zhou, "Multi-objective path planning for UAV in the urban environment based on CDNSGA-II," in *Proceedings of 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 2019, pp. 350–3505.

[24] J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," *CoRR*, vol. abs/1804.02767, 2018.

[25] G. Cheng, J. Han, and X. Lu, "Remote sensing image scene classification: Benchmark and state of the art," *Proceedings of the IEEE*, vol. 105, no. 10, pp. 1865–1883, 2017.

[26] G.-S. Xia, J. Hu, F. Hu, B. Shi, X. Bai, Y. Zhong, L. Zhang, and X. Lu, "AID: A benchmark data set for performance evaluation of aerial scene classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 55, no. 7, pp. 3965–3981, 2017.

[27] J. A. Fernandes and J. C. Neves, "Angle invariance for distance measurements using a single camera," in *Proceedings of 2006 IEEE International Symposium on Industrial Electronics*, vol. 1, 2006, pp. 676–680.

[28] S. J. Burian, S. P. Velugubantla, K. Chittineni, S. R. K. Maddula, and M. J. Brown, "Morphological analyses using 3D building databases: Portland, Oregon," Utah. LA-UR, Los Alamos National Laboratory, Los Alamos, NM, Tech. Rep., 2002.

[29] A. Hidalgo-Panagua, M. A. Vega-Rodríguez, J. Ferruz, and N. Pavón, "Solving the multi-objective path planning problem in mobile robotics with a firefly-based approach," *Soft Computing*, vol. 21, no. 4, pp. 949–964, 2017.